LISTING OF THE CLAIMS

1. (Currently Amended) A computer network intrusion detection system comprising:

a plurality of different log analyzers for different external networks, each log analyzer being configured for detecting attacks upon a firewall in an corresponding one of the different external networks defining an edge detection network;

an edge database log coupled to the different log analyzers logging attacks upon the different external networks;

an intrusion detector coupled to a client network and configured to ~~for~~ detect~~ing~~ external attacks upon ~~a computer~~ the client network;

an analyzer coupled to said intrusion detector for analyzing each detected attack and determining a characteristic indicative thereof to classify each detected attack as a general attack or a client specific attack based upon logged attacks in the edge database log; and

a filter coupled to said analyzer for generating an alert based upon characteristics of a plurality of attacks.

2. (Original) The system according to claim 1 wherein said filter generates a first alert signal in response to an attack having a new characteristic, and further generates a second alert signal indicative of a predetermined plurality of attacks having the new characteristic occurring within a predetermined time.

3. (Original) The system according to claim 1 wherein said filter generates a first alert signal in response to an attack having a new characteristic, and further generates a subsequent first alert signal in response to a subsequent attack having the new characteristic occurring after an absence of attacks having the new characteristic occurring within a predetermined time.

4. (Original) The system according to claim 1 wherein said filter generates the alert in response to attacks of a predetermined characteristic exceeding a predetermined rate or frequency.

5. (Original) The system according to claim 4 wherein the predetermined rate or frequency deterministically varies.

6. (Original) The system according to claim 1 further comprising a second intrusion detector for detecting attacks upon a second computer network, wherein said filter is further coupled to said second intrusion detector and communicates the alert to the computer network in response to attacks of a predetermined characteristic upon the second computer network exceeding a predetermined rate or frequency.

7. (Original) The system according to claim 1 further comprising:

a vulnerability tester coupled to said analyzer for testing a second computer network for a vulnerability to an attack characteristic detected by said analyzer.

8. (Original) The system according to claim 1 further comprising:

an second intrusion detector for detecting external attacks upon a second computer network;

a second analyzer coupled to said second intrusion detector for analyzing each detected attack upon the second network and determining a characteristic indicative thereof, wherein said filter is further coupled to said second analyzer and further compares the attack characteristics determined by said analyzer and said second analyzer and generates a general attack alert in response to a substantial similarity in the comparison.

9. (Original) The system according to claim 1 further comprising:

a second intrusion detector for detecting external attacks upon a second computer network;

a second analyzer coupled to said second intrusion detector for analyzing each detected attack upon the second network and determining a characteristic indicative thereof, wherein said filter is further coupled to said second analyzer and further compares the attack characteristics determined by said analyzer and said second analyzer and generates a specific attack alert in response to a substantial absence of similarity in the comparison.

10. (Original) The system according to claim 9 further comprising an alert generator for generating an alert indicative of the specific attack on the one of the

networks experiencing the attacks having the absence of similarity of attacks on the other of the networks.

11. (Original) The system according to claim 9 further comprising: a vulnerability tester coupled to said filter for testing the one of the networks not experiencing the attacks for a vulnerability to the attack characteristic experienced by the other of the computer networks.

12. (Proposed Amended) A method of generating a network intrusion alert for a first network coupled to a multiple client network system comprising the steps of:

logging attacks on multiple different external networks defining an edge detection network;

detecting an attack on a client network;

classifying the attack as either a general attack or a client specific attack by comparing the attack to attacks logged for the edge detection network;

~~determining a characteristic of an attack upon the first network;~~

~~determining if the characteristic matches a characteristic of an attack upon a second client coupled to the multiple client network system~~; and

prioritizing handling of the detected attack if the attack is classified as a general attack

~~generating a first alert in response to an absence of the match~~.

13. (Original) The method according to claim 12 further comprising the step of generating a second alert in response to the presence of the match.

14. (Original) The method according to claim 13 wherein the first alert is indicative of a specific attack on the first network and the second alert is indicative of a non-specific attack on the first network.

15. (Original) The method according to claim 12 wherein said step of determining if the characteristic matches a characteristic of an attack upon a second client determines if the characteristic matches a characteristic of attacks upon multiple clients coupled to the multiple client network system.

16. (Currently Amended) A method of preempting an intrusion comprising the steps of:

determining characteristics of an attack upon a plurality of firewalls for individual external ~~first~~ hosts in an edge detection network; and

internally testing a client ~~second~~ host outside of the edge detection network for a susceptibility to an attack of the determined characteristics for the attack upon the firewalls for the individual external hosts in the edge detection network.

17. (Original) The method according to claim 16 further comprising the step of further determining if the characteristic of the attack upon the first host is a new characteristic, wherein said step of testing does not test the susceptibility of the second

host if said step of further determining does not determine that the characteristic of the attack upon the first host corresponds to the new characteristic.

18. (Original) The method according to claim 17 wherein the new characteristic corresponds to a characteristic not previously determined.

19. (Original) The method according to claim 16 further comprising the step of generating an alert if said step of testing indicates that the second host is susceptible to the determined characteristics.

20. (Original) The method according to claim 16 further comprising the step of filtering the determined characteristics of a plurality of attacks determined by said step of determining and generating an alert signal in response to a substantial increase in frequency or rate of attacks of the characteristic, wherein said step of testing tests the susceptibility of the second host in response to the alert signal.